SYSTEM AND METHOD FOR PROVIDING CONFIGURABLE SECURITY MONITORING UTILIZING AN INTEGRATED INFORMATION SYSTEM

Cross-Reference to Related Application

This application claims the benefit of U.S. Provisional Application No. 60/236,282 filed on September 28, 2000, the benefit of which is hereby claimed under U.S.C. § 119. U.S. Provisional Application No. 60/236,282 is incorporated by reference herein.

Field of the Invention

The present invention relates generally to a security monitoring network and, in particular, to a system and method for providing variable, remote monitoring of a locally detected event utilizing an integrated information system.

Background of the Invention

Generally described, electronic security systems are configured to provide a wide range of security services in both residential and commercial settings. The types of monitoring devices utilized by a particular security system to perform the system service depend greatly on the sophistication of the security system configuration and the overall function of the security system. A majority of conventional security systems include intrusion detecting devices, such as door or window contacts, glass break detectors, motion detectors and the like. In a commercial setting, closed-circuit television ("CCTV"), badging systems, asset tracking, and access control devices and sensors are also utilized.

The configuration of the security system is based on the function the system will serve. For example, in one aspect, a typical electronic security system may be used to provide smoke, fire, and/or carbon monoxide detection. Accordingly, the

system would utilize one or more smoke, fire and/or carbon monoxide detectors within one or more locations on the premises. In another aspect, the security system may also be utilized to provide motion or access detection as well as general video and audio monitoring of the premises. Accordingly, the system would utilize ingress or egress sensors and/or video cameras within the premises.

While the conventional art generally discloses utilizing multiple monitoring devices to perform various functions, conventional systems are deficient in data management functionality and integration. Security data from different monitoring device types is generally not integrated to affect the system reporting and control. Instead, the conventional security system is built around independent stand-alone devices that require human control and interpretation.

In one security configuration, contract or in-house security guard and patrol services are employed in a range of industrial commercial, public and private settings. The primary functions of the security guard may include direct visual surveillance, the monitoring of security cameras or other security devices, a reception or access control and authorization function, and incident response. A security guard may also be used to monitor a number of CCTV screens arranged in a bank formation. Accordingly, the security guard accepts the variety of inputs and makes a determination of a security alert, such as an unauthorized entrance.

The use of dedicated monitoring services, such as security guards is generally prohibitively expensive and unavailable for a majority of individuals and businesses. Additionally, if the guard is distracted, absent or inattentive, a security event may go unreported. Furthermore, the monitoring device data, such as the CCTV data, is typically available only to the dedicated premises monitor and cannot be utilized concurrently by additional users, such as a remote monitor, a quality control supervisor, the owner of the premises, or emergency or public safety authorities. Moreover, a single security guard may not be capable of processing all of the possible monitoring data sources simultaneously, thereby reducing the effectiveness of multiple monitoring devices.

Another security system configuration utilizes external monitors to provide the security services. Generally described, external monitoring systems are more cost effective than a dedicated on-premises monitor. However, most external monitoring systems have a limited effectiveness in being unable to extensively provide and/or review detailed security information. For example, most conventional external monitoring systems cannot incur the expense of providing a sufficient

amount of communication bandwidth to transmit continuous video/audio feeds from every monitored premises. Accordingly, if the external monitoring service detects an unauthorized entry into a premises, such as through a signal from a detecting device, the monitoring service typically dispatches emergency or public safety authorities to investigate and determine the extent of the detected event. In a vast majority of cases, the alarm is false and the premises owner incurs a fine for having the authorities verify the incident. Additionally, in the event of an actual emergency, the monitoring service cannot provide the public safety authorities with sufficient information to assess the situation with monitoring devices, thereby putting the authorities at greater risk.

Similar to the dedicated on-premises monitoring, the remote monitoring service also cannot concurrently process the device information to multiple authorized users for various purposes. For example, a premises owner may need to access video data to locate a pet within the premises, while emergency or public safety personnel would need to access the same video data to identify the location of a victim. In both cases, the monitoring service likely cannot provide the information to the user on a wide scale basis.

Some conventional security system configurations attempt to integrate at least some security monitoring devices to better detect alarm conditions from a remote user. For example, a security system monitor (either remote or on-premises) may detect an unauthorized entry from a motion detector and confirm it by utilizing a video camera. Generally however, these systems are directed towards a combination of video surveillance and are limited into being processed solely for the detection of an intrusion or the verification of an intrusion. These systems generally cannot accept additional non-security information inputs that relate generally to the management of the premises and that are outside of the scope of conventional security monitoring. Moreover, these systems are deficient in that the data cannot be processed concurrently or distributed to multiple authorized users.

In addition to the above-mentioned deficiencies in the conventional art, some monitoring systems, either with a on-premises guard or an external monitor, are further deficient in creating an uncomfortable environment by monitoring (and often recording) on a continuous basis. For example, it may be advantageous to have video access to a public restroom in the event of a medical emergency. However, one skilled in the relevant art will appreciate that the constant monitoring of a public restroom creates an uncomfortable environment for patrons utilizing the facilities

during non-emergencies. Additionally, continuous monitoring of areas not prone to have a high rate of emergencies quickly becomes expensive. For example, the constant monitoring of a parking lot during typically off-peak hours presents a great expense to a parking lot provider. Accordingly, many parking lots are left to be monitored by attendants that may have a variety of functions, such as collection, access control, etc.

Thus, there is a need for an integrated information system that can obtain any variety of monitoring device inputs, process any combination of the inputs, and provide customized outputs according to the needs and rights of an authorized user.

Summary of the Invention

A system and method for implementing an integrated information system are provided. A premises server is in communication with a variety of information sources that produce monitoring data for a premises. The information sources include subsidiary device servers, a variety of individual monitoring devices, as well as other network systems that produce data to be processed. The premises server collects, presents, and transmits monitoring device data to a central server capable of processing data from multiple premises servers. The central server receives the data and traverses one or more logical rule sets to determine whether the inputted data violates the rules. Based on an evaluation of the rules, the central server generates outputs in the form of communication to one or more authorized users via a variety of communication mediums and devices and/or the instigation of a variety of acts corresponding to the evaluation of the rules. Accordingly, the monitoring device data is processed and distributed on multiple levels by the integrated security system.

In one aspect of the present invention, a method for providing an integrated information system in a system having at least one monitoring device is provided. In accordance with the method, an integrated information system obtains monitoring device data from the at least one monitoring device. The integrated information system obtains one or more rules corresponding to the at least one monitoring device. The one or more rules establish a threshold for the monitoring device data. The integrated information system processes the monitoring device data according to the monitoring rules and generates an output corresponding to the processing of the monitoring device data. The output may include no output.

In another aspect of the present invention, a system for implementing an integrated information system is provided. The integrated information system includes one or more monitoring devices operable to transmit monitoring device data

and a central processing server operable to obtain the monitoring device data from the one or more monitoring devices. The central processing server processes the monitoring device data according to one or more monitoring device rules and generates an output corresponding to the processing, wherein the output may include no output.

In yet a further aspect of the present invention, a system for implementing an integrated information system is provided. The integrated information system includes one or more monitoring devices operable to transmit monitoring device data and central processing means for obtaining the monitoring device data from the one or more monitoring devices, processing the monitoring device data according to one or more monitoring device rules and generating outputs corresponding to the processing, wherein the outputs may include no output.

Brief Description of the Drawings

The foregoing aspects and many of the attendant advantages of this invention will become more readily appreciated as the same become better understood by reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

FIGURE 1 is a block diagram of an Internet environment;

FIGURE 2 is a block diagram of an integrated information system in accordance with the present invention;

FIGURE 3 is a block diagram depicting an illustrative architecture for a premises server in accordance with the present invention;

FIGURE 4 is a block diagram depicting an illustrative architecture for a central server in accordance with the present invention;

FIGURE 5 is a flow diagram illustrative of a monitoring device data processing routine in accordance with the present invention;

FIGURE 6 is a flow diagram illustrative of a device event processing subroutine in accordance with the present invention;

FIGURES 7A and 7B are flow diagrams illustrating an asset/resource event processing subroutine in accordance with the present invention;

FIGURE 8 is illustrative of a screen display produced by a WWW browser enabling a user to review a monitoring device rule in accordance with the present invention;

FIGURE 9 is illustrative of a screen display produced by a WWW browser enabling a user to review integrated information system data logs in accordance with the present invention;

FIGURE 10 is an exemplary user interface screen display illustrating a message management interface in accordance with the present invention.

Detailed Description of the Preferred Embodiment

As described above, aspects of the present invention are embodied in a World Wide Web (the "WWW" or "web") site accessible via the Internet. As is well known to those skilled in the art, the term "Internet" refers to the collection of networks and routers that use the Transmission Control Protocol/Internet Protocol ("TCP/IP") to communicate with one another. A representative section of the Internet 20 is shown in FIGURE 1, in which a plurality of local area networks ("LANs") 24 and a wide area network ("WAN") 26 are interconnected by routers 22. The routers 22 are special purpose computers used to interface one LAN or WAN to another. Communication links within the LANs may be twisted wire pair, or coaxial cable, while communication links between networks may utilize 56 Kbps analog telephone lines, 1 Mbps digital T-1 lines, 45 Mbps T-3 lines or other communications links known to those skilled in the art. Furthermore, computers and other related electronic devices can be remotely connected to either the LANs 24 or the WAN 26 via a modem and temporary telephone or wireless link. It will be appreciated that the Internet 20 comprises a vast number of such interconnected networks, computers, and routers and that only a small, representative section of the Internet 20 is shown in FIGURE 1. One skilled in the relevant art will appreciate that aspects of the present invention may be practiced on Internet networks, such as an Intranet.

The Internet has recently seen explosive growth by virtue of its ability to link computers located throughout the world. As the Internet has grown, so has the WWW. As is appreciated by those skilled in the art, the WWW is a vast collection of interconnected or "hypertext" documents written in HyperText Markup Language ("HTML"), or other markup languages, that are electronically stored at "WWW sites" or "Web sites" throughout the Internet. A WWW site is a server connected to the Internet that has mass storage facilities for storing hypertext documents and that runs administrative software for handling requests for those stored hypertext documents. A hypertext document normally includes a number of hyperlinks, i.e., highlighted portions of text which link the document to another hypertext document possibly stored at a WWW site elsewhere on the Internet. Each hyperlink is associated with a

Uniform Resource Locator ("URL") that provides the exact location of the linked document on a server connected to the Internet and describes the document. Thus, whenever a hypertext document is retrieved from any WWW server, the document is considered to be retrieved from the WWW. As is known to those skilled in the art, a WWW server may also include facilities for storing and transmitting application programs, such as application programs written in the JAVA® programming language from Sun Microsystems, for execution on a remote computer. Likewise, a WWW server may also include facilities for executing scripts and other application programs on the WWW server itself.

A consumer or other remote consumer may retrieve hypertext documents from the WWW via a WWW browser application program. A WWW browser, such as Netscape's NAVIGATOR® or Microsoft's Internet Explorer, is a software application program for providing a graphical consumer interface to the WWW. Upon request from the consumer via the WWW browser, the WWW browser accesses and retrieves the desired hypertext document from the appropriate WWW server using the URL for the document and a protocol known as HyperText Transfer Protocol ("HTTP"). HTTP is a higher-level protocol than TCP/IP and is designed specifically for the requirements of the WWW. It is used on top of TCP/IP to transfer hypertext documents between servers and clients. The WWW browser may also retrieve application programs from the WWW server, such as JAVA applets, for execution on the client computer.

Referring now to FIGURE 2, an actual embodiment of an integrated information system 30 in accordance with the present invention will be described. An integrated information system 30 is a subscriber-based system allowing a number of monitoring devices within one or more premises to be processed at a single control location. Additionally, the data from the monitoring devices is processed according to one or more rules. The control location customizes output of the processed data to a number of authorized users dependent on the preferences and rights of the user. While the system of the present invention is utilized to integrate traditional security monitoring functions, it is also utilized to integrate any information input in a like manner.

With reference to FIGURE 2, the integrated information system 30 includes a premises server 32 located on a premises. The premises server 32 communicates with one or more monitoring devices 34. As illustrated in FIGURE 2, the premises server 32 communicates with the monitoring devices 34 via a network connection. A

more detailed description of a network for communicating with monitoring devices, including the use of one or more device servers, is found in co-pending U.S. Provisional Application No. _____, entitled SYSTEM AND METHOD FOR MANAGING A DEVICE NETWORK, filed April 3, 2001, the disclosure of which is hereby incorporated by reference.

In an illustrative embodiment, the monitoring devices 34 can include smoke, fire and carbon monoxide detectors. The monitoring devices 34 can also include door and window access detectors, glass break detectors, motion detectors, audio detectors and/or infrared detectors. Still further, the monitoring devices 34 can include computer network monitors, voice identification devices, video cameras, still cameras, microphones and/or fingerprint, facial, retinal, or other biometric identification devices. Still further, the monitoring devices 34 can include conventional panic buttons, global positioning satellite ("GPS") locators, other geographic locators, medical indicators, and vehicle information systems. The monitoring devices 34 can also be integrated with other existing information systems, such as inventory control systems, accounting systems, or the like. It will be apparent to one skilled in the relevant art that additional or alternative monitoring devices 34 may be practiced with the present invention.

The premises server 32 also communicates with one or more output devices 36. In an illustrative embodiment, the output devices 36 can include audio speakers, display or other audio/visual displays. The output devices 36 may also include electrical or electro-mechanical devices that allow the system to perform actions. The output devices 36 can include computer system interfaces, telephone interfaces, wireless interfaces, door and window locking mechanisms, aerosol sprayers, and the like. As will be readily understood by one skilled in the art, the type of output device is associated primarily with the type of action the information system 30 produces. Accordingly, additional or alternative output devices 36 are considered to be within the scope of the present invention. In accordance with the present invention, the monitoring devices 34 and the output devices 36 can be linked together in a computer network environment in which multiple premises servers 32 work in parallel, sharing data and processes. Moreover, additional premises servers 32, monitoring devices 34, and output devices 36 may be joined modularly to provide extensibility to the system.

FIGURE 3 is a block diagram depicting an illustrative architecture for a premises server 32. Those of ordinary skill in the art will appreciate that the

premises server 32 includes many more components then those shown in FIGURE 3. However, it is not necessary that all of these generally conventional components be shown in order to disclose an illustrative embodiment for practicing the present invention. As shown in FIGURE 3, the premises server 32 includes a network interface 38 for connecting directly to a LAN or a WAN, or for connecting remotely to a LAN or WAN. Those of ordinary skill in the art will appreciate that the network includes the necessary circuitry for such a connection, and is also constructed for use with the TCP/IP protocol, the particular network configuration of the LAN or WAN it is connecting to, and a particular type of coupling medium. The premises server 32 may also be equipped with a modem for connecting to the Internet through a point to point protocol ("PPP") connection or a serial line Internet protocol ("SLIP") connection as known to those skilled in the art.

The premises server 32 also includes a processing unit 40, a display 42, an input/output (I/O) interface 44 and a mass memory 46, all connected via a communication bus, or other communication device. The I/O interface 44 includes hardware and software components that facilitate interaction with a variety of the monitoring devices via a variety of communication protocols including TCP/IP, X10, digital I/O, RS-232, RS-485 and the like. Additionally, the I/O interface 44 facilitates communication via a variety of communication mediums including telephone land lines, wireless networks (including cellular, digital and radio networks), cable networks and the like. In an actual embodiment of the present invention, the I/O interface is implemented as a layer between the server hardware and software applications utilized to control the individual monitoring devices. It will be understood by one skilled in the relevant art that alternative interface configurations may be practiced with the present invention.

The mass memory 46 generally comprises a RAM, ROM, and a permanent mass storage device, such as a hard disk drive, tape drive, optical drive, floppy disk drive, or combination thereof. The mass memory 46 stores an operating system 48 for controlling the operation of the premises server. It will appreciated that this component may comprises a general-purpose server operating system as is known to those skilled in the art, such as UNIX, LINUX™, or Microsoft WINDOWS NT®. The memory also includes a WWW browser 50, such as Netscape's NAVIGATOR® or Microsoft's Internet Explorer browsers, for accessing the WWW.

The mass memory 46 also stores program code and data for interfacing with various premises monitoring devices, for processing the monitoring device data and

for transmitting the data to a central server. More specifically, the mass memory stores a device interface application 52 in accordance with the present invention for obtaining monitoring device data from a variety of devices and for manipulating the data for processing by the central server. The device interface application 52 comprises computer-executable instructions which, when executed by the premises server 32 obtains and transmits device data as will be explained below in greater detail. The mass memory 46 also stores a data transmittal application program 54 for transmitting the device data to a central server and to facilitate communication between the central server and the monitoring devices 34. The operation of the data transmittal application 54 will be described in greater detail below. It will be appreciated that these components may be stored on a computer-readable medium and loaded into the memory of the premises server using a drive mechanism associated with the computer-readable medium, such as a floppy, CD-ROM, DVD-ROM drive, or network drive.

Returning to FIGURE 2, the premises server 32 is in communication with a central server 56. Generally described, the central server 56 obtains various monitoring device data, processes the data and outputs the data to one or more authorized users. In an illustrative embodiment, the communication between the central server 56 and the premises server 32 is remote and two-way. FIGURE 4 is a block diagram depicting an illustrative architecture for a central server 56. Those of ordinary skill in the art will appreciate that the central server 56 includes many more components then those shown in FIGURE 4. However, it is not necessary that all of these generally conventional components be shown in order to disclose an illustrative embodiment for practicing the present invention.

As shown in FIGURE 4, the central server 56 includes a network interface 58 for connecting directly to a LAN or a WAN, or for connecting remotely to a LAN or WAN. Those of ordinary skill in the art will appreciate that the network interface includes the necessary circuitry for such a connection, and is also constructed for use with the TCP/IP protocol, the particular network configuration of the LAN or WAN it is connecting to, and a particular type of coupling medium. The central server 56 may also be equipped with a modem for connecting to the Internet 20.

The central server 56 also includes a processing unit 60, a display 62 and a mass memory 64, all connected via a communication bus, or other communication device. The mass memory 64 generally comprises a RAM, ROM, and a permanent mass storage device, such as a hard disk drive, tape drive, optical drive, floppy disk

drive, or combination thereof. The mass memory 64 stores an operating system 66 for controlling the operation of the central server. It will appreciated that this component may comprises a general-purpose server operating system.

The mass memory 64 also stores program code and data for interfacing with the premises devices, for processing the device data and for interfacing with various authorized users. More specifically, the mass memory 64 stores a premises interface application 68 in accordance with the present invention for obtaining data from a variety of monitoring devices and for communicating with the premises server. The premises interface application 68 comprises computer-executable instructions which, when executed by the central server 56, interfaces with the premises server 32 as will be explained below in greater detail. The mass memory 64 also stores a data processing application 70 for processing monitoring device data in accordance with rules maintained within the central server. The operation of the data processing application 70 will be described in greater detail below. The mass memory 64 further stores an authorized user interface application 72 for outputting the processed monitoring device data to a variety of authorized users in accordance with the security process of the present invention. The operation of the authorized user interface application 72 will be described in greater detail below. It will be appreciated that these components may be stored on a computer-readable medium and loaded into the memory of the central server using a drive mechanism associated with the computer-readable medium.

It will be understood by one skilled in the relevant art that the premises server 32 may be remote from the premises or may omitted altogether. In such an alternative embodiment, the monitoring devices 34 transmit the monitoring data to a remote premises server 32 or alternatively, they transmit the monitoring data directly to the central server 56.

Also in communication with the central server 56 is a central database 74. In an illustrative embodiment, the central database 74 includes a variety of databases including an event logs database 76, an asset rules database 78, a resource rules database 80, an asset inventory database 82, a resource inventory database 84, an event rules database 86 and an active events database 88. The utilization of the individual databases within the central database 74 will be explained in greater detail below. As will be readily understood by one skilled in the relevant art, the central database 74 may be one or more databases, which may be remote from one another.

Additionally, it will be further understood that one or more of the databases 74 may be maintained outside of the central server 56.

With continued reference to FIGURE 2, the central server 56 communicates with one or more notification acceptors 90. In an illustrative embodiment, the notification acceptors 90 include one or more authorized users. Each authorized user has a preference of notification means as well as rights to the raw and processed monitoring data. The authorized users include premises owners, security directors or administrators, on-site security guards, technicians, remote monitors (including certified and non-certified monitors), customer service representatives, emergency personnel and others. As will be readily understood by one skilled in the art, various user authorizations may be practiced with the present invention. Additionally, it will be further understood that one or more of the rules databases may be maintained outside of the central server.

In an illustrative embodiment of the present invention, the central server 56 communicates with the notification acceptors 90 utilizing various communication devices and communication mediums. The devices include personal computers, hand-held computing devices, wireless application protocol enabled wireless devices, cellular or digital telephones, digital pagers, and the like. Moreover, the central server 56 may communicate with these devices via the Internet 20 utilizing electronic messaging or Web access, via wireless transmissions utilizing the wireless application protocol, short message services, audio transmission, and the like. As will be readily understood by one skilled in the art, the specific implementation of the communication mediums may require additional or alternative components to be practiced. All are considered to be within the scope of practicing the present invention.

Generally described, the present invention facilitates the collection and processing of a variety of premises information for distribution to one or more authorized users in a highly extensible manner. The system of the present invention obtains monitoring data from any one of a variety of monitoring devices 34. In an actual embodiment of the present invention, the monitoring device data is categorized as asset data, resource data or event data. Asset data is obtained from a monitoring device corresponding to an identifiable object that is not capable of independent action. For example, asset data includes data obtained from a bar code or transponder identifying a particular object, such as a computer, in a particular location. Resource data is obtained from a monitoring device corresponding to an

identifiable object that is capable of independent action. For example, resource data includes data from a magnetic card reader that identifies a particular person who has entered the premises. Event data is obtained from a monitoring device corresponding to an on/off state that is not correlated to an identifiable object. Event data is a default category for all of the monitoring devices. As will be readily understood by one skilled in the relevant art, alternative data categorizations are considered to be within the scope of the present invention.

The monitoring device data is obtained by the monitoring devices 34 on the premises server 32 and transmitted to the central server 56. The central server 56 receives the monitoring device data and processes the data according to a rules-based decision support logic. In an actual embodiment of the present invention, the central server 56 maintains databases 74 having logic rules for asset data, resource data and event data. Moreover, because the monitoring device data is potentially applicable to more than one authorized user, multiple rules may be applied to the same monitoring device data. In an alternative embodiment, the rules databases 74 may be maintained in locations remote from the central server 56.

In the event the processing of the monitoring device rules indicates that action is required, the central server 56 generates one or more outputs associated with the rules. The outputs include communication with indicated notification acceptors 90 according to the monitoring device data rules. For example, an authorized user may indicate a hierarchy of communication mediums (such as pager, mobile telephone, land-line telephone) that should be utilized in attempting to contact the user. The rules may also indicate contingency contacts in the event the authorized user cannot be contacted. Additionally, the rules may limit the type and/or amount of data to which the user is allowed to access. Furthermore, the outputs can include the initiation of actions by the central server 56 in response to the processing of the rules.

FIGURE 5 is a flow diagram illustrative of a device decision support process support routine 500 for processing the monitoring device data in accordance with the present invention. At block 502, the central server 56 obtains an input from a monitoring device. In an actual embodiment of the present invention, the input is obtained from the premises server 32. Alternatively, the input may be received directly from the monitoring device 34 or the central server 56 may poll individual devices (or the premises server 32) for an input. At block 504, the central server 56 identifies the device processing the data. The identification may be accomplished by determining a network address from which the input originated and which is assigned

to the specific devices, or by reading other identification data that can be included with the data input.

At decision block 506, a test is performed to determine whether the device data includes intelligence data. In an actual embodiment of the present invention, the intelligence data includes data that characterizes the data as asset data or resource data, because the data contains information identifying the object. In contrast, data that does not contain any information identifying an object and is not considered intelligent. If the device is not determined to be intelligent or if the device cannot be identified, at block 508, an event log database 76 is updated to reflect the input data. At block 510, the central server 56 processes the data according to a process device event subroutine. The routine 500 terminates at block 512.

FIGURE 6 is a flow diagram illustrative of a process device event subroutine 600 in accordance with the present invention. At block 602, the central server 56 obtains the monitoring device rules. In an actual embodiment, the monitoring device rules are stored in a database 86 in communication with the central server 56. The rules contain data indicating one or more ranges for determining a rule violation. In a broad sense, a rule violation is an indication of an event occurrence for which a notification is required. The ranges correspond to the type of data produced by the monitoring device. For example, if a monitoring device 34 is capable of only two stages (e.g., on or off), the rule may indicate that existence of one stage, e.g. "on", is a violation. The rules may also include an indication that one or more monitoring device rules must also be considered before the rule is determined to be violated. For example, a rule corresponding to a glass break detector may indicate that a motion detector signal must be detected before the rule is violated. As will be readily understood by one skilled in the relevant art, additional or alternative rule types are considered to be within the scope of the present invention.

At decision block 604 a test is performed to determine whether a device rule is found. If no rule is found, the process terminates at block 606. If, however, a device rule is found, at block 608 the central server 56 evaluates the rule according to the data received from the monitoring device 34. In an illustrative embodiment, the rules may include preset or default rules maintained by the central server 56. Additionally, the rules may include independently created rules by one or more authorized users. Moreover, one or more authorized users may be given the authority to modify or update rules via a user interface.

At decision block 610, a test is performed to determine whether the device rule is violated. If the rule is violated, at block 612, the central server 56 creates a rule violation output. In an actual embodiment of the present invention, the rules violation output instructions are included in the rule. The instructions include a list of the authorized users to notify in the event of a rule violation and a hierarchy of which communication medium and devices should be utilized to contact each authorized user. For example, the rules may be in the form of logical if/then statements implementing an iterative hierarchy for establishing communication with an authorized user. Moreover, the instructions may also indicate the extent of the data that that authorized user has access to. For example, the output may include the generation of a call to the premises owner's mobile device, the paging of an on-site monitor and a land-line telephone call to the public authorities. Alternatively, the central server may also maintain an output database indicating the output instructions corresponding to each rule.

In addition to generating communications, the rules violation output may also instigate an integrated system response. For example, in the case of an intrusion, a dye may be sprayed on the intruder from an aerosol sprayer. Additionally, the system may sound an audible alarm and directly dial emergency personnel. In another example, if the system rules violation is a medical emergency, the central server 56 may call an ambulance, turn on lights within the premises, and unlock the doors to facilitate entry by the emergency personnel.

Once the central server 56 has generated the rules violation output at block 612 or if the event rule is not violated at block 610, the subroutine 600 terminates at block 614.

Returning to FIGURE 5, if at block 506, the device data includes intelligence information, at block 514, the intelligence is translated from the monitoring device data. At block 516, the log event database 76 is updated to reflect the input data. At block 518, the central server 56 processes the data according to a process asset/resource event subroutine. The routine 500 terminates at block 520.

FIGURES 7A and 7B are flow diagrams illustrative of a process asset or resource event subroutine 700 in accordance with the present invention. With reference to FIGURE 7A, at decision block 702, a test is performed to determine whether the input signal is asset data. If the signal is identified as asset data, at block 704, the asset rules are obtained. In an actual embodiment of the present invention, the asset rules are maintained and retrieved from an asset rules

database 78. At block 706, a test is performed to determine whether an asset rule is found. If no asset rule is found for the asset, the monitoring device data is processed as a device event at block 708. In an actual application of the present invention, the device event is processed as described above with respect to the device event processing subroutine 600 (FIGURE 6). In an illustrative embodiment of the present application, in the event the asset rule processing cannot be completed, the monitoring device is still processed as a device-level event.

If an asset rule is found, at decision block 710, a test is performed to determine whether the asset rule is violated. In an actual embodiment of the present invention, the asset rule contains data allowing the central server 56 to determine a rule violation. For example, an asset rule may contain information indicating a requirement of both a particular object (e.g., a computer) performing an action (e.g., logged into a network) for a violation. Additionally, the asset rule may indicate that additional device, resource or asset rules may be considered prior to determining whether the rule has been violated. As explained above, the rules may include preset rules maintained by the central server and user implemented/modified rules.

If the rule has not been violated, the monitoring device data is processed as a device event at block 708. It will be generally understood by one skilled in the relevant art, that processing the rule as a both an asset and a device event allows for multiple purpose processing of the monitoring device data, such as the detection of a specific object and the detection of an object.

If the asset rule has been violated, at block 712, the central server 56 reads a known asset inventory to identify the asset. In an actual embodiment of the present invention, central server maintains and reads from an asset inventory database 82. At decision block 714, a test is performed to determine whether the asset is found in the asset inventory. If the asset is not found, the system defaults to processing the monitoring device data as a device event at block 708. If the asset is found in the asset inventory, at block 716, central server 56 outputs the asset violation. In an actual embodiment of the present invention, the asset rule contains instructions for generating output in the event of a rule violation to one or more authorized users. The instructions also contain a hierarchy of communication mediums and communication devices to attempt to contact the authorized user. Additionally, the instructions may contain alternative contact personnel if central server cannot contact the authorized user. Moreover, as explained above, the output may also instigate

action by the integrated system. At block 708, the monitoring device data is processed as a device event.

With reference to FIGURE 7B, if the signal is not determined to be asset data at block 702 (FIGURE 7A), at decision block 718, a test is done to determine whether the inputted signal is resource data. If the signal is not identified as resource data, at block 720, the monitoring device data is processed as a device event. In an actual application of the present invention, the device event is processed as described above with respect to the device event processing subroutine 600 (FIGURE 6). If the signal is identified as resource data, at block 722, the resource rules are obtained. In an actual embodiment of the present invention, the resource rules are maintained and retrieved from a resource rules database 80. At block 724, a test is performed to determine whether a resource rule is found. If no resource rule is found for the resource, the monitoring device data is processed as a device event at block 726.

If a resource rule is found, at decision block 728, a test is performed to determine whether the resource rule is violated. In an actual embodiment of the present invention, the resource rule contains data allowing the central server to determine a rule violation. Additionally, the resource rule may indicate that additional device, resource or asset rules may be considered prior to determining whether the rule has been violated. If the rule has not been violated, at block 726, the monitoring device data is processed as a device event. It will be generally understood by one skilled in the relevant art, that processing the rule as a both a resource and a device event allows for multiple purpose processing of the monitoring device data.

If the resource rule has been violated, at block 730, the central server 56 reads a known resource inventory to identify the resource. In an actual embodiment of the present invention, central server 56 maintains and reads from a resource inventory database 84. At decision block 732, a test is performed to determine whether the resource is found in the resource inventory. If the resource is not found, the system defaults to processing the monitoring device data as a device event at block 726. If the resource is found in the resource inventory, at block 734, central server 56 outputs the resource violation. In an actual embodiment of the present invention, the resource rule contains instructions for generating output in the event of a rule violation to one or more authorized users. The instructions also contain a hierarchy of communication mediums and communication devices to attempt to contact the authorized user. Additionally, the instructions may contain alternative contact

personnel if central server 56 cannot contact the authorized user. Moreover, as explained above, the output may also instigate action by the integrated system. At block 726, the monitoring device data is processed as a device event.

FIGURES 8, 9, and 10 are exemplary screen displays illustrative of various user interfaces relating to various aspects of the integrated information system 10 of the present invention. In an illustrative embodiment of the present invention, the various user interfaces allows an authorized system user to perform a variety of tasks associated with the integrated information system 10 including, but not limited to, installing new monitoring devices 34 or output devices 36, generating or modifying device, asset and resources rules, and/or reviewing collected data. One skilled in the relevant art will appreciate that a variety of user interfaces may be utilized in conjunction with the present invention and that the disclosed embodiments are illustrative and should not be construed as limiting.

In an actual embodiment of the present invention, portions of a user interface with the integrated information system 30 are displayed remotely from one or more of the servers. For example, an authorized user, such as the premises owner, may be available to view an event violation remotely through the use of a standard Internet Web browser based connection. In another embodiment, a remote monitoring service may be given access to control one or more of the monitoring devices 34 via a Web browser based connection or via a direct communication line. Still further, security personnel may review real time monitoring device 34 data via a wireless communication device. Accordingly, the user interface provided to the authorized user may conform to the function being performed, the limits of a device, or the communication medium transmitting the data.

FIGURE 8 is illustrative of a screen display 92 produced by a WWW browser enabling a user to review a monitoring device rule in accordance with the present invention. As illustrated in FIGURE 8, the screen display 92 includes a field 94 for identifying a name for the rule, one or more fields 96 identifying rule attributes, and one or more fields 98 identifying the notification attributes in the event there is a rule violation. In an actual embodiment of the present invention, an authorized user may review the rule detail, and may also modify or create new rules by completing the associated in the fields.

FIGURE 9 is illustrative of a screen display 100 produced by a WWW browser enabling a user to review integrated information system 10 data logs in accordance with the present invention. In an actual embodiment of the present

invention, the integrated information system 30 may keep a central log for all event, device and resource violations. As illustrated in FIGURE 9, the screen display 100 provides the user with a table 102 of all rules violation data collected by the integrated information system 10. In the illustrative embodiment of the present invention, the table 102 includes a variety of records 104 that include a premises identifier field 105, a time stamp field 106, a device location field 107, a monitoring device 34 identifier field 108, a data descriptor field 110, and an indication 112 of whether the data includes video data. In an actual embodiment of the present invention, an authorized user can filter through the event log by specify searching criteria. Additionally, the authorized user may view more detailed information about specific records 104 by manipulating a peripheral graphical device interface tool, such as a mouse or by using a touchscreen interface. One skilled in the relevant art will appreciate that the event log table 102 may be modified to include additional or less fields.

FIGURE 10 is illustrative of a screen display 114 produced by a WWW browser enabling a user to review integrated information system 10 event data logs in accordance with the present invention. In addition to the table 102 of all rules violation, the integrated information system 30 may also maintain specific tables of event rule violations, device rule violations and resource rules violations. The screen display 114 illustrated in FIGURE 10 includes a table 116 of all event rules violation data. The table 116 is defined by a variety of records 118 that are defined by a client premises location field 120, an event status field 122, a time stamp field 124, an event severity field 126, an event location field 128, a device identifier field 130, a device location field 132 and a video data present field 134. Similar to the screen display 100, in an actual embodiment of the present invention, an authorized user is able to filter event data and also obtain greater detail. One skilled in the relevant art will appreciate that various screen display formats may be utilized with the present invention.

In an illustrative embodiment of the present invention, the method and system of the present invention are implemented in the form of a computer network monitor. It will be understood by one skilled in the relevant art that the disclosed illustrative embodiment is done by way of example and that the present invention is not limited to its application as a computer network monitor. In accordance with the illustrative embodiment, the premises server is connected to a computer network monitor associated with a premises computer network. The computer network monitor serves

as a resource data detector by identifying one or more specific users who are logged onto the computer network. Additionally, the computer network monitor serves as an asset data detector by identifying one or more specific network components, such as mass memory storage or servers, on the computer network. Finally, the computer network monitor serves as a event data detector by identifying how many users are logged into the network or that a user is logged onto the network.

In accordance with this embodiment, a computer network monitoring device collects information regarding the identity of users logged into the network. The monitor may also collect information regarding network usage, or inactivity. The central server obtains the network monitor data and obtains a resource rule corresponding to an identified resource. In the illustrative embodiment, the central server the resource rule may dictate whether the user is authorized to log into the network from a particular computer or whether the user is allowed to log into the computer network at certain times. For example, a rule may indicate a user may not be allowed to log into the network from a computer outside of the premises. Similarly, the rule may indicate that the user may not log into the network after 8:00 p.m. Moreover, the resource rule (reflective of the fact that the user is on vacation) may indicate that the user is not be logged in to the network at all.

In the event that the resource rule is violated, the central server contacts the authorized users, such as a computer system administrator, listed in the resource rule and may also disconnect the user. The central server may also instigate action, such as logging the user off the network automatically.

The computer system monitor data may also be processed as an asset data event. In this capacity, if one of the network components is in need of maintenance (e.g., disk full or server down), the central server indicates a rules violation and generates an appropriate output. Another asset rule application may include detecting when a specific component is used (thereby creating a rules violation) for tracking system utilization.

The computer system monitor data may also be processed as a device event indicating that another user is logged into the network. In this capacity, a device event rule within the central server may indicate a rule violation if more than twenty users are logged in at the same time. Accordingly, irrespective of whether the resource rule is violated, an event rule may also be violated by the same action. Thus, the security system processes the data according to several rules and issues notifications according to each rule.

In another illustrative embodiment of the present invention, the method and system of the present invention are implemented in the form of a premises access control system. It will be understood by one skilled in the relevant art that the disclosed illustrative embodiment is done by way of example and that the present invention is not limited to its application as a premises access detection system. In accordance with the illustrative embodiment, the premises server is connected to one or more presence indicators, such as a magnetic identification card reader, video camera, and microphone. The premises access monitor serves as a resource data detector by identifying one or more persons who enter the premises. Additionally, the premises access monitor serves as a event data detector by identifying that one or more persons are present, irrespective of the identity of the person.

In one aspect, the central server obtains the monitoring device data and obtains a resource rule corresponding to an identified resource. In the illustrative embodiment, the resource rule may dictate whether the user is authorized to enter specific areas of the premises or whether the user is authorized to be in a specific area at a certain time of day. For example, a resource rule may state that the particular user may not be allowed to enter the computer room without a computer administrator, whose presence is determined by another resource rule, also being in the room. The user may also not be allowed to enter a file room after 8:00 p.m.

In another aspect of this illustrative embodiment, the monitoring device data may include an audible signal, such as a call for "help." Utilizing voice recognition software, the system can process the words to initiate an action according to the rules. For example, the system may be trained to respond to all persons who state an "emergency" word, such as "help." Additionally, the system may respond to authorized users, whose voice print can be identified, allowing the user additional control or access to the system.

In addition to being processed as a resource rule, the computer system monitor data may also be processed as a device event indicating that a person, regardless of the identity on the premises. In this capacity, a device event rule within the central server may indicate a rule violation if anyone is in a certain area. Accordingly, irrespective of whether the resource rule is violated, an event rule may also be violated by the same action.

In the event that either a resource rule and/or event rule is violated, the central server contacts the authorized users, such as a security monitor to indicate an unauthorized person on the premises. The device processing server may also

instigate action, such as sounding an audible alarm or locking secured areas of the premises. In one aspect of this illustrative embodiment, the premises server may instigate a two-way conversation with a person on the premises, or create a three-way telephone call. In another aspect of this illustrative embodiment, the rule violation may instigate the recording of the monitoring device data. Accordingly, an authorized user, such as the premises owner, has the opportunity to view the data, through a Web browser. The authorized user can utilize the data to confirm a security event or for informative purposes.

In another alternative application of this illustrative embodiment, an authorized system user needs to contact someone currently on the premises. Accordingly, the system would poll the premises server to obtain the identity of the persons on the premises. The authorized user would request information regarding the presence of particular people or anyone in general. The system could also identify a closest communication device associated with the person on the premises to contact the particular person. Moreover, in the event public safety personnel are contacted and are given limited authority to the system, the system may output the identity and location of the unauthorized person on the premises to the authorities via a mobile device or a video display.

In another aspect of the present invention, the transmission of the monitoring device data and output data is facilitated through standard communication mediums, such as the Internet. However, the use of standard communication channels creates a need for data security and integrity. For example, in the case of conventional video transmission over the Internet, such as streaming, loss of video data is common and utilized to reduce data size. As will be generally understood by one skilled in the relevant art, however, the loss of video frame data for detecting a security event is generally unacceptable.

The present invention overcomes the deficiencies by implementing a packet encrypted data transmission method. In accordance with this aspect of the present invention, the premises server packages the monitoring device data into smaller sized data packets. Each data packet is compressed, encrypted and sent to the device processing server over the Internet. The central server obtains the packet and decrypts the data. The data is processed and an acknowledge signal is sent to the premises server. The premises server then is ready to send the next package. If the data cannot be processed or appears to be compromised, the central server will not acknowledge the packet. Accordingly, the premises server will either try to resend

the packet or fail the transmission. As will be readily understood by one skilled in the art, the method is also utilized to transmit data from the central server to the premises server or to a notification acceptor.

The encrypted package transmission method of the present invention allows the security network to utilize standard communication channels, while mitigating the security risks associated with those channels. Moreover, the method further mitigates the loss of data in transmitting the data through the security network.

The present invention facilitates the integration of a variety of monitoring devices such that monitored data may be processed by a system applying multiple rules. By evaluating the monitored data by one or more rules having different outputs, the same monitoring data may be utilized by different authorized users, having different access rights, for different purposes. This also allows the system to be customized for different privacy regulations.

In yet another aspect of the present invention, the integrated information system 10 is implemented to provide support to an unlimited number of devices in a single distributed data network. In this embodiment, the multiple premises server computers 32, monitoring devices 34, and output devices 36 are linked together in a computer network and associated into a single logical connector. Accordingly, the processing of the monitoring device data may be distributed over any number of premises servers 32. Additionally, a distributed network environment provides a modularity to system. The modularity allows for expansion and/or reconfiguration of the integrated information.

Other examples of potential uses of the system of the present invention include, but are not limited to, integration with an electronic inventory system to process a low inventory event. Additionally, the system maybe integrated with many household appliances to allow a service call to be made when the appliance needs repair. The system may also allow for integrating security monitoring devices to allow a guard to "patrol" the premises by concurrently utilizing multiple devices, such as access detectors, cameras and microphones. As will be readily understood, numerous additional uses may also be practiced with the present invention.

While an illustrative embodiment of the invention has been illustrated and described, it will be appreciated that various changes can be made therein without departing from the spirit and scope of the invention.